(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2003069644 A
(43) Date of publication of application: 07.03.2003

(51) Int. Cl H04L 12/56
G06F 13/00, H04M 3/00

(21) Application number: 2001258398
(22) Date of filing: 28.08.2001

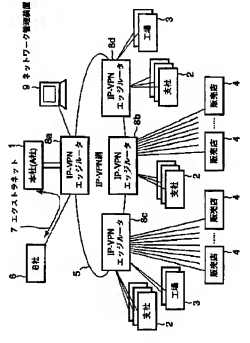
(71) Applicant: TOSHIBA CORP
(72) Inventor: WATANABE MASANORI

(54) NETWORK MANAGEMENT DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To realize a service which monitors the present network operation state to predict the future tendency and presents it to clients.

SOLUTION: A network management device 9 connected to an IP-VPN (virtual private network) network 5 constructed as an enterprise network is provided with a function which periodically collects information required for quality management like a transmission/reception traffic volume from an edge router set as a management object out of IP-VPN edge routers 8a, 8b, 8c and 8d of the IP-VPN network 5 and predicts the tendency of the future operation condition like transition of future traffic and reports the prediction result. Thus, smooth network extension and update or change of service like QoS (quality of service) can be proposed to clients to prevent a lack of bands and the degradation in quality in the future.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－69644
（P2003－69644A）
(43)公開日　平成15年３月７日(2003.3.7)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/56	４００	Ｈ０４Ｌ　12/56	４００Ｂ	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５３	Ｇ０６Ｆ　13/00	３５３Ｂ	５Ｋ０３０
Ｈ０４Ｍ　3/00		Ｈ０４Ｍ　3/00	Ｄ	５Ｋ０５１

審査請求　未請求　請求項の数７　ＯＬ　（全９頁）

(21)出願番号　特願2001－258398(P2001－258398)

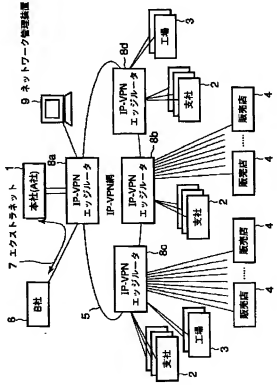
(22)出願日　平成13年８月28日(2001.8.28)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　渡辺　正衛
東京都府中市東芝町１番地　株式会社東芝
府中事業所内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　５Ｂ０８９　ＪＡ３５　ＪＢ１４　ＫＡ１３
５Ｋ０３０　ＧＡ１４　ＨＡ０８　ＨＢ１１　ＨＣ０１　ＨＣ１３
ＨＤ０３　ＪＡ１０　ＪＬ０７　ＫＡ０５　ＭＡ０１
ＭＡ０４　ＭＢ０２　ＭＢ０９　ＭＣ０７　ＭＣ０８
５Ｋ０５１　ＣＣ０８　ＤＤ０３　ＦＦ０１　ＦＦ０３

(54)【発明の名称】　ネットワーク管理装置

(57)【要約】
【課題】現在のネットワーク運用状態を監視して今後の動向を予測して顧客に提示するサービスを実現する。
【解決手段】企業網として構築されたＩＰ－ＶＰＮ網５のＩＰ－ＶＰＮエッジルータ８ａ、８ｂ、８ｃ、８ｄの中で管理対象として設定されたエッジルータからから送受信トラヒック量などの品質管理に必要な情報を定期的に収集し、将来のトラヒックの推移など今後の運用状況の動向を予測し、その予測結果を通知する機能をＩＰ－ＶＰＮ網５に接続されたネットワーク管理装置９に備える。これにより、顧客に対してスムーズなネットワークの拡張やＱｏＳなどのサービスの更新、変更を提案でき、将来の帯域不足や品質低下を未然に防ぐことができる。



1

【特許請求の範囲】

【請求項１】　企業網として各拠点間を結ぶ特定のネットワークに接続されて、上記ネットワークの運用状態を監視するネットワーク管理装置であって、

上記各拠点と上記ネットワークとの間に介在して上記企業に関するデータを論理的に他のデータと分離してルーティング処理する各ルータのうち、管理対象として設定されたルータから品質管理に必要な情報を定期的に収集する情報収集手段と、

この情報収集手段により収集された情報を解析して今後のネットワーク運用状態の動向を予測する予測手段と、

この予測手段によって予測された結果を通知する通知手段とを具備したことを特徴とするネットワーク管理装置。

【請求項２】　企業網として各拠点間を結ぶ特定のネットワークに接続されて、上記ネットワークの運用状態を監視するネットワーク管理装置であって、

上記各拠点と上記ネットワークとの間に介在して上記企業に関するデータを論理的に他のデータと分離してルーティング処理する各ルータのうち、管理対象として設定されたルータから少なくとも送受信トラヒック量を定期的に収集する情報収集手段と、

この情報収集手段により収集された送受信トラヒック量を解析して今後のトラヒック量の増減を予測する予測手段と、

この予測手段によって予測された結果を通知する通知手段とを具備したことを特徴とするネットワーク管理装置。

【請求項３】　上記通知手段は、上記予測手段により契約時に保証されたトラヒック量を超過すると判定された場合にその旨を通知することを特徴とする請求項２記載のネットワーク管理装置。

【請求項４】　企業網として各拠点間を結ぶ特定のネットワークに接続されて、上記ネットワークの運用状態を監視するネットワーク管理装置であって、

上記各拠点と上記ネットワークとの間に介在して上記企業に関するデータを論理的に他のデータと分離してルーティング処理する各ルータのうち、管理対象として設定されたルータから品質サービスを利用している送信元アドレスと送信先アドレスのペア数、それらの送受信トラヒック量を定期的に収集する情報収集手段と、

この情報収集手段により収集された送信元アドレスと送信先アドレスのペア数、送受信トラヒック量を解析して今後のサービス利用状況を予測する予測手段と、

この予測手段により予測された結果を通知する通知手段とを具備したことを特徴とするネットワーク管理装置。

【請求項５】　上記通知手段は、上記予測手段により契約時に保証されたサービス品質を低下すると判定された場合にその旨を通知することを特徴とする請求項４記載のネットワーク管理装置。

2

【請求項６】　企業網として各拠点間を結ぶ特定のネットワークに接続されて、上記ネットワークの運用状態を監視するネットワーク管理装置であって、

上記各拠点と上記ネットワークとの間に介在して上記企業に関するデータを論理的に他のデータと分離してルーティング処理する各ルータのうち、管理対象として設定されたルータから品質サービスの各クラス毎の送受信トラヒック量、各クラスでのポート番号毎の送受信トラヒック量を定期的に収集する情報収集手段と、

この情報収集手段により収集された各クラス毎の送受信トラヒック量、各クラスでのポート番号毎の送受信トラヒック量を解析して、今後のサービス利用状況を各クラス別に予測する予測手段と、

この予測手段によって予測された結果を通知する通知手段とを具備したことを特徴とするネットワーク管理装置。

【請求項７】　上記通知手段は、上記予測手段により契約時に保証されたサービス品質を低下するクラスがあると判定された場合にその旨を通知することを特徴とする請求項６記載のネットワーク管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、企業の拠点間を結ぶネットワークの運用状態を管理するネットワーク管理装置に関する。

【０００２】

【従来の技術】従来の企業ネットワークは、求められる品質、安定度の高さ、さらにセキュリティーの観点から専用線を使用したネットワーク構築が一般的であった。しかし、インターネットの普及、インターネットのバックボーンの帯域、品質の進歩、インターネット上で仮想的に企業網（ＶＰＮ：Virtual Private Network）を構築する技術の確立により、多くの企業が自社の広域ネットワークをインターネット上に構築しようとしている。これにより、企業網の中、遠距離の転送に要するコストを大幅に削減することが可能になり、通信事業者が提供するアウトソーシングサービスを利用すれば、更なるコストの削減が図れることから今後も多くの企業がＶＰＮの導入を進める傾向にある。

【０００３】この通信事業者が提供するＶＰＮには、暗号化によりセキュリティーを考慮したインターネットＶＰＮと呼ばれるものや、暗号化によるセキュリティーだけではなく、インターネット上を転送される他のトラヒックと論理的に分離することによって、より高いセキュリティーを提供し、さらに専用線のような高い品質を実現するＩＰ－ＶＰＮなどがある。

【０００４】ＩＰ－ＶＰＮとは、通信事業者の閉域ＩＰネットワーク網を通信経路として用いる仮想専用網のことであり、複数のプロバイダのネットワークを経由する必要があるインターネットを用いないため、エンド・ト

ゥ・エンドで機密性や通信品質に優れたＩＰ接続が行える。

【０００５】ここで、ＩＰ－ＶＰＮサービスでは、帯域や品質、セキュリティーなど、顧客の多様な要求に対応すべく様々なオプションが用意されており、これらをどのように選択するかは、各企業にあったネットワークの設計によって決定される。企業が企業網の一新、もしくは変更を行うなど、新たなネットワークを設計する上でもっとも必要となるのは、現状のネットワークの運用状態の調査とその解析、今後のトラヒックの予測であり、それらを基にその帯域や品質（トラヒック量や転送レートなど）を決定する。これらの情報が正確であればあるほど、新ネットワークに移行した後の安定的な運用が保証され、トラブルの発生を抑えることができる。

【０００６】しかし、ネットワークに接続する端末、拠点の増加とともにそのネットワーク設計が複雑化しており、ネットワークの運用状態の調査、解析、将来のトラヒックの予測は困難で、正確に行おうとすれば多くの時間と費用を要することになる。また、ネットワーク全般の技術革新も著しく、その調査、解析および予測に時間を掛けすぎると、次から次へと出てくる新たなサービスに対応できなくなってしまう。かといって、不充分な調査結果、予測でネットワークを設計してしまうと、導入後のトラブル等で再度詳細な調査、解析が必要となり、多大な損失を生んでしまう。

【０００７】また、近年のネットワーク技術者の慢性的な不足などにより、企業網の自営が困難となってきており、通信事業者のアウトソーシングサービスを選択する企業が現れており、今後この流れは加速するものと予測される。アウトソーシングサービスを提供する通信事業者としても、運用状態の正確な調査、解析、将来のトラヒックの増加の予測は、将来のトラブルを回避するために必須ではあるが、ある程度の運用状態の監視は行っているものの、常に将来のトラヒックを念頭においての運用監視は行えていないのが現状である。

【０００８】

【発明が解決しようとする課題】上述したように、従来、企業網を新規もしくは変更する時点で、企業は独自に、もしくは通信事業者やコンサルティング会社等に依頼して現状の運用状態を監視することはあるが、それは単にトラブルが発生していないかという観点からの監視であって、将来のネットワークを設計する上で参考となる情報を収集しているものではない。

【０００９】なお、ネットワークの品質を管理するものとして、特開２００１－６９１７０号公報の「品質予測値提示通信網」が知られている。しかしながら、上記公報では、品質が保証されていないオープンなネットワークを前提とし、ルータ間のリンクのトラヒック情報に基づいて遅延や損失の少ないデータの転送経路（ルート）を検証するものであって、上述したＩＰ－ＶＰＮのように品質が保証された閉域ネットワークによって構築された企業網を対象として、現在のネットワーク運用状態を監視することはできない。

【００１０】そこで、本発明は、品質が保証されたネットワークにより企業網が構築されている場合において、現在のネットワーク運用状態を監視して今後の動向を予測して顧客に提示するサービスを実現するネットワーク管理装置を提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明のネットワーク管理装置は、企業網として各拠点間を結ぶ特定のネットワークに接続されて、上記ネットワークの運用状態を監視するネットワーク管理装置であって、上記拠点と上記ネットワークとの間に介在して上記企業に関するデータを論理的に他のデータと分離してルーティング処理する各ルータのうち、管理対象として設定されたルータから品質管理に必要な情報を定期的に収集する情報収集手段と、この情報収集手段により収集された情報を解析して今後のネットワーク運用状態の動向を予測する予測手段と、この予測手段によって予測された結果を通知する通知手段とを具備して構成される。

【００１２】このような構成のネットワーク管理装置によれば、企業網を構成するネットワーク上の各ルータの中で管理対象として設定されたルータから品質管理に必要な情報が本装置によって定期的に収集される。上記品質管理に必要な情報とは、例えば当該ルータにおける送受信トラヒック量である。このようにして収集された情報から今後のネットワーク運用状態の動向が予測されて通知される。すなわち、例えば現在のトラヒック量から今後のトラヒック量の増減が予測されて、契約時に保証されたトラヒック量を超過するような場合にその旨が通知される。したがって、管理者はその通知を受けることで、顧客にネットワークの拡張などを提案でき、将来の帯域不足や品質低下のトラブルを未然に防ぐことができると共に、顧客側では企業網の運用状態がより正確に把握できるため、スムーズな契約の更改を行うことができる。

【００１３】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態を説明する。

【００１４】図１は本発明の一実施形態に係るネットワーク構成を示す図であり、ＩＰ－ＶＰＮサービスを使用したＡ社の企業網の一例が示されている。

【００１５】図１において、Ａ社は、本社１と、全国に点在する多数の支社２、工場３および販売店４などを結んで企業網としてのＩＰ－ＶＰＮ網５を構築している。また、ＩＰ－ＶＰＮ網５内のＮＡＴ（Network Address Translator）を利用して提携会社であるＢ社とのエクストラネット７も構築している。

【００１６】通信事業者が提供するＩＰ－ＶＰＮサービ

スは、インターネット上に論理的に切り離されたネットワークを構築し、それを企業網の中、長距離のデータ転送路とする。図１では、ＩＰ－ＶＰＮエッジルータ８ａ、８ｂ、８ｃ、８ｄ間がこれに当たる。これらのＩＰ－ＶＰＮエッジルータ８ａ、８ｂ、８ｃ、８ｄは、キャリア側のネットワークと顧客側のネットワークとの間に介在し、特にＩＰ－ＶＰＮでは暗号化やトンネリングなどによって他のデータと論理的に分離してルーティング処理を行う機能を有する。

【００１７】ＩＰ－ＶＰＮ網５で結ばれた本社１、支社２、工場３、販売店４の各拠点は、それぞれに対応したＩＰ－ＶＰＮエッジルータ８ａ、８ｂ、８ｃ、８ｄに接続されており、例えば高速デジタル回線（ＨＳＤ：High Super Digital）、ＡＴＭ（Asynchronous Transfer Mode）専用線、ＦＲ（Frame Relay）回線、ＩＳＤＮ（Integrated Services Digital Network）回線などを利用してＩＰ－ＶＰＮ網５にアクセスする。

【００１８】また、このＩＰ－ＶＰＮ網５には、ＩＰ－ＶＰＮエッジルータ８ａを介して本発明のネットワーク管理装置９が接続されている。このネットワーク管理装置９は、ＩＰ－ＶＰＮ網５に設けられた各ＩＰ－ＶＰＮエッジルータ８ａ、８ｂ、８ｃ、８ｄから定期的に品質管理に必要な情報を収集して蓄積し、その収集、蓄積された情報を分析して今後の運用状態の動向を予測する機能を備える。

【００１９】このような構成において、Ａ社の企業網の運用状態を調査する場合には、その企業網を構成するＩＰ－ＶＰＮエッジルータ８ａ、８ｂ、８ｃ、８ｄの動作状態を管理することが重要となる。なお、ＩＰ－ＶＰＮエッジルータ８ａ、８ｂ、８ｃ、８ｄ間には、ＩＰ－ＶＰＮサービスの基幹となるバックボーンに図示せぬＩＰ－ＶＰＮコアルータが多数存在している。このＩＰ－ＶＰＮコアルータはＩＰ－ＶＰＮエッジルータ８で集約されたデータを転送するものであり、別の顧客からのデータも含まれる。したがって、そこでの情報からはＡ社の企業網に関する運用状態を解析するには精度の粗いものとなるため、ここではＩＰ－ＶＰＮコアルータは管理対象外としている。

【００２０】一般的に本社１、支社２、工場４などは頻繁に増減するものではないが、販売店４ともなると頻繁にその数が増減することが考えられる。また、経理システムなどのアプリケーションを新しいものに変更する場合には、全社一斉に変更するケースが多く、アプリケーション自体が一斉に変更されるため、転送されるパケットの品質も激変することも考えられる。

【００２１】このようなことを考慮すると、Ａ社の企業網の運用状態の調査では、ＩＰ－ＶＰＮエッジルータ８ａ、８ｂ、８ｃ、８ｄから以下のような項目に関する情報を定期的に収集する必要がある。

【００２２】・Ｕｐ－ｓｔｒｅａｍ（アクセス側からバックボーン側）のトラヒック量
・Ｄｏｗｎ－ｓｔｒｅａｍ（バックボーン側からアクセス側）のトラヒック量
・アクセス側のルーティングキャッシュの送信元アドレス数
・アクセス側のルーティングキャッシュの送信先アドレス数
・バックボーン側のルーティングキャッシュの送信元アドレス数
・バックボーン側のルーティングキャッシュの送信先アドレス数
・アプリケーション毎のＵｐ－ｓｔｒｅａｍの送受信トラヒック量
・アプリケーション毎のＤｏｗｎ－ｓｔｒｅａｍの送受信トラヒック量
・各品質レベル毎のＵｐ－ｓｔｒｅａｍの送受信トラヒック量および廃棄トラヒック量
・各品質レベル毎のＤｏｗｎ－ｓｔｒｅａｍの送受信トラヒック量および廃棄トラヒック量
・ＩＰ－ＶＰＮ網内の各種ＮＡＴとの送受信トラヒック量

などである。

【００２３】これらの情報を定期的に収集して解析することにより、企業網全体の現状の運用状態を把握でき、その時間的推移を検証することにより、将来のトラヒックの推移など今後の運用状態の動向を予測することが可能となる。

【００２４】すなわち、例えば、アクセス側の端末数やどのアプリケーションのデータ転送が増加しているのか、ＮＡＴを使ってのインターネットアクセスがどの程度増加しているのか、エクストラネットでのデータ転送がどのくらい増えているのかなど、そのネットワークの変動状況が判明する。これらの情報の収集、解析、予測は図１のネットワーク管理装置９にて行われる。

【００２５】ネットワーク管理装置９には、ＳＮＭＰ（Simple Network Management Protocol）といったネットワーク管理プロトコルが使用されている。ＳＮＭＰは、ＴＣＰ／ＩＰネットワークでネットワーク管理システムを構成するためのプロトコルであり、ネットワークに接続されたルータやブリッジなどの各種管理対象となるネットワーク構成機器（エージェントと呼ばれる）から管理に必要な情報を授受する方法が規定されている。

【００２６】図１の例では、ＩＰ－ＶＰＮエッジルータ８ａ、８ｂ、８ｃ、８ｄの中で管理対象として設定された任意のＩＰ－ＶＰＮエッジルータから収集した所定の情報を元に、例えば１ヵ月後、３ヵ月後、半年後、１年後というように、将来の企業網の運用状態の予測を行うシステムがネットワーク管理装置９に搭載されており、それをスムーズなネットワークの拡張、新規ネットワークの設計に役立たせるものである。

【００２７】以下に、具体例を挙げて説明する。

【００２８】例えば、図２に示すように、ＩＰ－ＶＰＮエッジルータ８ｂに接続された支店２や販売店４からＩＰ－ＶＰＮ網５を介してＩＰ－ＶＰＮエッジルータ８ａに接続された本社１の顧客登録サーバ１０へアクセスする場合において、高い品質での通信を保証するＱｏＳ（Quality of service）サービスを利用しているケースを考える。ＱｏＳとは、ネットワークのサービス品質のことであり、ＯＳＩ参照モデルではネットワーク層（第３層）で規定されており、例えば音声や動画などの一定の帯域が必要なアプリケーションやリアルタイム性を要求する通信に優先的に帯域を割り当てるなどの制御を行う。

【００２９】Ａ社は、本社１と全支店２、全販売店４で使用する顧客登録のアプリケーションの使用頻度が高く、高いレスポンスを要求することから、これらに関するデータの転送に対し、優先度の高いトラヒックの帯域を優先的に確保、転送するＱｏＳサービスを５Ｍｂｐｓの帯域だけ契約しているものとする。図２に示すＩＰ－ＶＰＮエッジルータ８ａ、８ｂ（ルータＡとルータＢ）には、このＱｏＳサービスを利用するトラヒックを他のトラヒックと分離するために、その送信元アドレスと送信先アドレスが登録されている。そして、ＩＰ－ＶＰＮエッジルータ８ｂが支社２から本社１へのデータを受信した際に、その受信したデータの送信元アドレスと送信先アドレスがＱｏＳサービス用として予め登録された送信元アドレスと送信先アドレスに該当するか否かをチェックする。そして、ＱｏＳサービスに該当する場合には、そのデータにＱｏＳの高いデータを示すフラグを付けてＩＰ－ＶＰＮエッジルータ８ａへ転送する。それを受信したＩＰ－ＶＰＮエッジルータ８ａは、上記フラグに基づいて当該データを優先的に本社１の顧客登録サーバ１０に転送する。本社１から支社２へのデータ転送時についても同様である。

【００３０】＜ケース１＞ここで、上記図２のようなケースでは、ＱｏＳサービスの利用によるデータの転送状態を監視するためには、ネットワーク管理装置９では、本社１に接続されたＩＰ－ＶＰＮエッジルータ８ａから以下のような情報を収集する。

【００３１】・ＱｏＳサービスを利用している送信元アドレスと送信先アドレスのペアの数
・ＱｏＳサービスを利用している各通信の送受信トラヒック量
これらの情報を定期的に収集した結果、ネットワーク管理装置９には、図３に示すような情報が蓄積される。図３の例では、２００１年１月２１日～同年４月２１日までの３ヶ月間に亘って一定時間間隔（３０分間隔）でＩＰ－ＶＰＮエッジルータ８ａから情報を収集した場合のＱｏｓ利用数、Ｑｏｓ利用時の送信トラヒック量と受信トラヒック量との関係が示されている。

【００３２】この情報収集結果から現状のＱｏＳサービスの利用状況を具体的に把握することが可能になり、ＱｏＳサービスを利用するクライアントの台数の推移とそのトラヒック量の推移から以下のようなことを解析できる。

【００３３】（１）２００１．１．２１から２００１．４．２１の３ヶ月間で、ＱｏＳサービスを利用しているクライアントの数が最大７１から８３に増加している。
（２）２００１．１．２１から２００１．４．２１の３ヶ月間で、ＱｏＳサービスを利用しているクライアントからサーバ方向のトラヒック量が平均１．００３１倍に増加している。
（３）２００１．１．２１から２００１．４．２１の３ヶ月間で、ＱｏＳサービスを利用しているサーバからクライアント方向のトラヒック量が平均１．００３２倍に増加している。

【００３４】以上のような解析結果から、例えば２ヶ月後の２００１．８．４には、ＱｏＳサービスを利用するトラヒックのうち、クライアントからサーバ方向のトラヒックが契約時の５Ｍｂｐｓを超える可能性が高くなることなどを予測することができる。

【００３５】このように、ネットワーク管理装置９はＩＰ－ＶＰＮエッジルータ８ａから収集した情報に基づいて、回帰計算などの所定の予測計算式を用いて今後の運用状態を予測する。その際、図４に示すようなトラヒック予測図を作成して、契約している帯域の超過や品質がＳＬＡ（Service Level Agreement：サービス品質保証契約）よりも低下することなどを予測した場合に、通信事業者の管理担当者に通知する。

【００３６】通知方法としては、特に限定されるものではないが、例えばネットワーク管理装置９に備えられているモニターに上記図４のトラヒック予測図を表示するとともに、将来、ＳＬＡより低下することが予測される場合にその旨をメッセージ表示するなどの方法がある。これを受けて、通信事業者は、顧客に対し、ネットワークの拡張や、新たなサービス内容の契約、変更を提案することで、帯域超過や品質の低下を未然に防ぐことができる。

【００３７】なお、図２の例では、本社１に対するアクセスを監視するためにＩＰ－ＶＰＮエッジルータ８ａを情報を収集するものとしたが、ＩＰ－ＶＰＮエッジルータ８ｂや他のＩＰ－ＶＰＮエッジルータに接続された支社２や販売店４などに対するアクセスを監視する場合には、上記同様にして、そこでのＩＰ－ＶＰＮエッジルータの情報を収集することで実現できる。どのルータを管理対象とするのかは管理項目に応じて決定される。ネットワーク管理装置９にはその管理対象として設定されたルータの位置情報が登録されており、ＩＰ－ＶＰＮエッジルータ８ａを起点にして当該ルータの情報を収集することになる。

【００３８】<ケース２>次に、図５に示すように、Ａ社の本社１と支社２との間に低、中、高の３つのＱｏＳのサービスクラスの帯域が契約されている場合を想定する。低クラスの帯域は５Ｍｂｐｓ、中クラスの帯域は１０Ｍｂｐｓ、高クラスの帯域は２０Ｍｂｐｓであり、これらのクラスはアプリケーションに応じて使い分けされている。アプリケーションとは、例えば経理システムなどであり、複数のアプリケーションを使用する場合には、各アプリケーションの使用頻度、重要度などに応じて図５のようにサービスクラスを分けることがある。

【００３９】ここで、ネットワーク管理装置９から以下のような情報をＩＰ－ＶＰＮエッジルータ８ａから収集する。

【００４０】・複数のサービスクラス毎の送受信トラヒック量
・各サービスクラスでＴＣＰ／ＵＤＰポート番号毎の送受信トラヒック量
ネットワーク管理装置９はこれらの情報を定期的に収集、蓄積することで、現状のＱｏＳサービスの利用状況を分析し、各サービスクラス毎にアプリケーションの推移とそのトラヒック量の推移から以下のような分析を行う。

【００４１】（１）２００１．１．２１から２００１．４．２１の３ヶ月間で、ＱｏＳサービス：高を利用している支社２から本社１向けのトラヒックが最大４．３Ｍｂｐｓから２．１Ｍｂｐｓに減少している。
（２）２００１．１．２１から２００１．４．２１の３ヶ月間で、ＱｏＳサービス：中を利用している支社２から本社１向けのトラヒックが最大６Ｍｂｐｓから８．７Ｍｂｐｓに増加している。
（３）２００１．１．２１から２００１．４．２１の３ヶ月間で、ＴＣＰ・Ｐｏｒｔ・Ｎｕｍｂｅｒ：６５３９の通信が１日平均１．０２１倍で増加している。

【００４２】以上のような分析結果から、例えば４５日後の２００１．６．５には、ＱｏＳサービス：中を利用するトラヒックのうち、支社２から本社８向けのトラヒックが契約している１０Ｍｂｐｓを超える可能性が高いと予測できる。

【００４３】また、既にＱｏＳサービスクラス：高を利用しているトラヒックが契約の５Ｍｂｐｓの５０％に到達することはなく、１５日後には契約帯域を２Ｍｂｐｓにしても十分運用可能であると予測できる。

【００４４】ネットワーク管理装置１は、このような予測の結果から現在の契約されている帯域の超過などを予測した場合に、通信事業者の管理担当者にその旨を通知する。

【００４５】上記ケース１、２のように、予測したいトラヒック量、品質に合わせて、測定するポイント、測定項目を選び、それらをネットワーク管理装置９で収集、蓄積、分析して予想を行うことで、将来のトラブルを未然に防ぐことができ、かつ、顧客の満足度の高いサービスを提供することが可能となる。

【００４６】また、上記ケース１、２以外には、以下のような例が考えられる。

【００４７】・ＩＰ－ＶＰＮエッジルータ８ａ、８ｂ、８ｃ、８ｄのそれぞれが転送しているトラヒック量を定期的に測定することにより、エッジルータ自身の転送能力の限界に達する時期を予測し、事前に、より転送能力の高い機器への変更を推奨する。

【００４８】・ＩＰ－ＶＰＮエッジルータ８ａ、８ｂ、８ｃ、８ｄにおけるＯＳＰＦ（OpenShortest path first）等のダイナミックルーティングプロトコルの情報パケットのロスなどを定期的に測定することにより、ルーティング情報の処理限界に達する時期を予測し、事前に、より処理能力の高い機器への変更、ルーティングのデザインの変更を推奨する。

【００４９】・ＮＡＴを経由するトラヒック量を定期的に測定することにより、現在使用中のＮＡＴのアドレス変換能力の限界に達する時期を予測し、事前に、より変換能力の高い機器への変更を推奨する。

【００５０】図６に上記の機能を実現するネットワーク管理装置９の処理の概要を示す。

【００５１】ネットワーク管理装置９は、情報収集機能部２１、情報蓄積部２２、トラヒック予測機能部２３、運用状態表示部２４を備えている。なお、このネットワーク管理装置９は、例えば磁気ディスク等の記録媒体に記録されたプログラムを読み込み、このプログラムによって動作が制御されるコンピュータによって実現される。

【００５２】統計情報収集機能部２１は、ＳＮＭＰ等のネットワーク管理プロトコルを使用して、ＩＰ－ＶＰＮ網５上の管理対象装置２０から各種情報を定期的に収集する。上記管理対象装置２０とは、図１のＩＰ－ＶＰＮ網５を構成する各ＩＰ－ＶＰＮエッジルータ８ａ、８ｂ、８ｃ、８ｄの中で管理対象として設定されたＩＰ－ＶＰＮエッジルータのことである。収集情報蓄積部２２は、情報収集機能部２１にて収集された情報を蓄積する。

【００５３】トラヒック予測機能部２３は、情報蓄積部２２に蓄積された情報を解析し、所定の計算式を用いて今後のトラヒックを予測し、その結果を情報蓄積部２２に送って蓄積する。このとき、予測されたトラヒックが契約時のトラヒックを越えるような場合に、トラヒック予測機能部２３はその旨を運用状態表示部２４を通じて管理者に通知する。

【００５４】管理者はその通知を受けると、予測されたトラヒックの情報を元にして帯域の拡張やＱｏＳなどの各種オプションの変更などを顧客に提案する。これにより、将来のトラブルを未然に防ぐことができると共に、通信事業者は契約内容の更新を効率的に行うことが可能

となる。また、このような予測結果を定期的に顧客に情報提供すれば、顧客側では自社の企業網の運用状態がより正確に把握できるため、スムーズな契約の更改を行うことができるようになる。

【００５５】

【発明の効果】以上詳記したように本発明によれば、品質が保証されたＩＰ－ＶＰＮなどの特定のネットワークにより構築された企業網において、ネットワーク上の管理対象として設定されたルータから品質管理に必要な情報を定期的に収集し、将来のトラヒックの推移など今後の運用状況の動向を予測し、その予測結果を通知する機能を同ネットワークに接続されたネットワーク管理装置に備えることで、顧客に対してスムーズなネットワークの拡張やＱｏＳなどのサービスの更新、変更を提案できる。これにより、将来の帯域不足や品質低下を未然に防ぐことが可能となり、通信事業者は予測結果を顧客に提供するサービスを行うことで、ネットワーク事業をさらに向上させることができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るネットワーク構成を示す図であり、ＩＰ－ＶＰＮサービスを使用した企業網の一例を示す図。

【図２】ＱｏＳサービスを利用している企業網の一例を＊示す図。

【図３】ＱｏＳサービス利用状況の情報収集結果を示す図。

【図４】情報収集結果に基づいて作成されたトラヒック予測図。

【図５】複数のクラス別にＱｏＳサービスを利用している企業網の一例を示す図。

【図６】本発明のネットワーク管理装置の処理機能を示すブロック図。

【符号の説明】

１～４…Ａ社の拠点

５…ＩＰ－ＶＰＮ網（Ａ社の企業網）

６…Ｂ社

７…エクストラネット

８ａ～８ｄ…ＩＰ－ＶＰＮエッジルータ

９…ネットワーク管理装置

１０…顧客登録サーバ

２０…管理対象装置（ＩＰ－ＶＰＮエッジルータ）

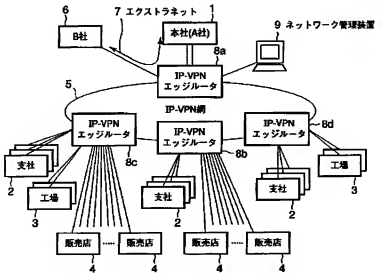
２１…情報収集機能部

２２…情報蓄積部

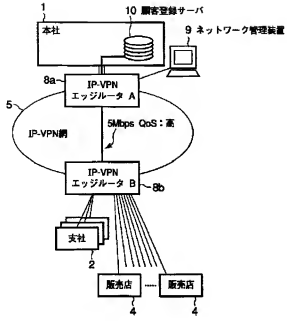
２３…トラヒック予測機能部

２４…運用状態表示部

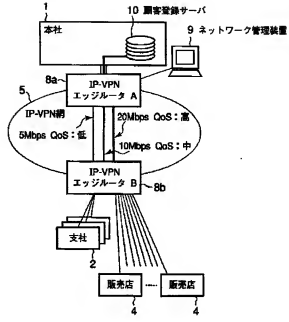
【図１】



【図２】



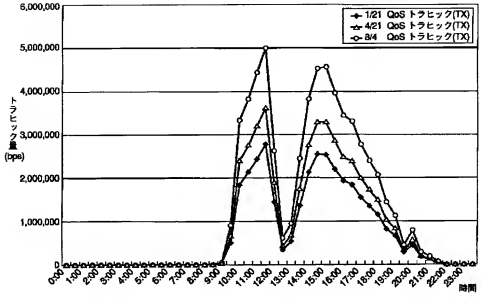
【図５】



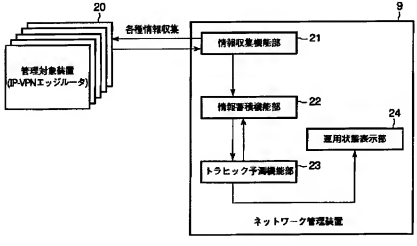
【図３】

Date	Time	QoS利用数	QoS利用トラヒック量(送信)	QoS利用トラヒック量(受信)
2001.1.21	10：00	58	1.843 Mbps	1.233 Mbps
	10：30	62	2.122 Mbps	1.443 Mbps
	11：00	66	2.431 Mbps	1.582 Mbps
	11：30	71	2.782 Mbps	1.873 Mbps
	12：00	41	1.440 Mbps	0.958 Mbps
	12：30	8	0.328 Mbps	0.253 Mbps
	13：00	15	0.525 Mbps	0.588 Mbps
⋮	⋮	⋮	⋮	⋮
2001.4.21	10：00	70	2.884 Mbps	2.042 Mbps
	10：30	74	3.211 Mbps	2.235 Mbps
	11：00	78	3.443 Mbps	2.433 Mbps
	11：30	83	3.611 Mbps	2.638 Mbps
	12：00	52	2.002 Mbps	1.433 Mbps
	12：30	11	0.503 Mbps	0.327 Mbps
	13：00	23	0.944 Mbps	0.766 Mbps

【図４】


1/21 QoS トラヒック(TX)
4/21 QoS トラヒック(TX)
8/4 QoS トラヒック(TX)
トラヒック量 (bps)
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
0:00
1:00
2:00
3:00
4:00
5:00
6:00
7:00
8:00
9:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
時間

【図６】


20
9
各種情報収集
管理対象装置
(IP-VPNエッジルータ)
情報収集機能部
21
情報蓄積機能部
22
24
運用状態表示部
トラヒック予測機能部
23
ネットワーク管理装置